Romaine C. Marshall (9654)
Engels J. Tejeda (11427)
HOLLAND & HART LLP
222 South Main Street, Suite 2200
Salt Lake City, UT 84101
Telephone: (801) 799-5800
rcmarshall@hollandhart.com
ejtejeda@hollandhart.com

Attorneys for Plaintiff Xat.com Limited

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, NORTHERN DIVISION

XAT.COM LIMITED, Plaintiff, v. HOSTING SERVICES, INC. A/K/A 100TB.COM, Defendant.	**COMPLAINT** Case No. 1:16-cv-00092 Honorable Paul M. Warner

Plaintiff Xat.com Limited ("Xat") alleges the following against Defendant Hosting Services, Inc., a/k/a 100TB.com ("100TB"):

PARTIES, JURISDICTION AND VENUE

1. Xat is a private limited company incorporated in the United Kingdom that has its principal place of business in the United Kingdom.

2. 100TB is a Delaware corporation that has its principal place of business in Providence, Utah.

3. The amount in controversy in this case, exclusive of interest and costs, exceeds the sum of $75,000.

4. This Court has diversity jurisdiction over the subject matter of this case pursuant to 28 U.S.C. § 1332(a)(2).

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391.

FACTUAL ALLEGATIONS

6. Xat is a social networking website where users exchange instant messages. As of the fall of 2015, Xat's website had approximately 1 million unique visitors and up to 40,000 active users in any 24-hour period.

7. On October 13, 2008, Xat retained 100TB to host Xat's servers. For this, the parties executed a Master Service Agreement ("MSA"), attached as Exhibit 1.

8. The MSA incorporates by reference 100TB's Privacy Policy, attached as Exhibit 2.

9. In Paragraph 4 of the MSA, 100TB represents that it has "received 'Safe Harbor' certification under U.S. – EU, and U.S. – Swiss safe harbor frameworks."

10. In its Privacy Policy, 100TB represents that it "complies with the U.S. – EU Safe Harbor Framework and the U.S. – Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce." It also certifies "that it adheres to both safe Harbor Privacy Principles' respective provisions addressing notice, choice, onward transfer, security, data integrity, access and enforcement."

11. Under the Safe Harbor Privacy Principles, "Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction."

12. In its Privacy Policy, 100TB represents that when individuals contact 100TB for support for their services, they will be asked to match certain information that is in their registration information.

13. Pursuant to the MSA, Xat was required to make monthly payments for services it received from 100TB. As of January 1, 2016, Xat was current on its payment obligations under the MSA.

14. Paragraph 7 of the MSA establishes a mechanism for termination of the MSA. As of January 1, 2016, neither party had terminated the MSA.

15. Under Paragraph 9 of the MSA, 100TB agrees to indemnify and hold Xat harmless from any and all third party actions, liability, damages, and costs and expenses, including attorneys' fees, arising from, or relating to, personal injury or property damage resulting from 100TB's gross negligence or willful misconduct.

16. On January 8, 2015, Xat warned 100TB that an unknown third party had requested that 100TB reset the password to Xat's servers and that the unknown third party appeared to be using "social engineering"[1] to con 100TB employees into changing the password to Xat's servers.

[1] "Social engineering" is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal procedures (e.g., obtaining the personal information of another person by intentionally misrepresenting a past or exiting fact).

17. 100TB responded to Xat's warning by representing to Xat that its password had not been reset.

18. Between January 14 and September 15, 2015, Xat received six notices that 100TB had received requests to reset Xat's password to its control panel. Xat communicated with 100TB regarding each of the unauthorized password reset requests, telling 100TB that they did not request any password resets.

19. On February 22, 2015, an unknown third party attempted to access Xat's servers through various means, including social engineering of 100TB's chat support group, and sending multiple "spoofed"[2] emails to 100TB requesting that 100TB change the password to Xat's servers.

20. On February 22, 2015, Xat informed 100TB that the spoofed emails were not sent by Xat and asked 100TB to confirm that 100TB would not act on any of the fraudulent requests for 100TB to change the password to Xat's servers.

21. On February 22, 2015, in spite of Xat's warnings and requests, 100TB changed the password for one of Xat's servers to a password provided by the unknown third party.

22. On February 23, 2015, Xat requested that 100TB investigate the security lapse of the prior day and that it involve its senior management in the matter to ensure it never happened again.

[2] Email "spoofing" is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source.

23. Between February 24 and March 11, 2015, 100TB requested that Xat implement an email-validation system on its email software called "Sender Policy Framework" ("SPF") on the assumption that Xat's email had been compromised.

24. Xat complied with 100TB's request by implementing SPF on its email, but informed 100TB that Xat's email had not been compromised and that adopting SPF would not prevent the types of attacks that had targeted its servers. Xat warned 100TB that the attacks targeted 100TB's systems and operations, not Xat's email system.

25. Between March 15 and September 16, 2015, an unknown third party contacted 100TB on multiple occasions requesting that 100TB alter the password to Xat's servers or add email addresses to Xat's account.

26. Each time that 100TB informed Xat that someone had requested a change to its servers' password, Xat warned 100TB that it did not make the request and that the request was instead an attempt to obtain unauthorized access – to hack – into Xat's servers.

27. On September 16, 2015, 100TB confirmed to Xat all of the unknown third-party attempts to access Xat's account were logged and retained in case that information was necessary for a subsequent investigation.

28. In the fall of 2015, 100TB offered "two-factor authentication" – a service whereby customers like Xat could enable a security measure that required two components (such as a password and a computer-generated personal identification number) to access their accounts.

29. On September 8, 2015, Xat enabled two-factor authentication for access to the control panels of its servers with 100TB.

30. On November 4, 2015, an unknown third party successfully convinced 100TB to add an unauthorized email address to Xat's account, to turn off two-factor authentication on Xat's account, and to give the unknown third-party control over Xat's servers (the "First Cyberattack").

31. During the First Cyberattack, the attacker(s) damaged one of Xat's servers, stole proprietary software, and wiped the server so that Xat was unable to recover data from it.

32. In response to the First Cyberattack, Xat requested that 100TB shut down its servers until Xat could receive assurances that the First Cyberattack had been contained.

33. In response to the First Cyberattack, Xat requested that 100TB back-up the servers to prevent loss of data in any future attack and that it verify that its servers were secured.

34. Following the First Cyberattack, Xat warned 100TB that the attackers were still trying to access Xat's servers and asked that 100TB confirm that the servers were locked down.

35. On information and belief, 100TB did not power-down at least three of Xat's servers after the First Cyberattack, did not turn on two-factor authentication, and did not backup the data on the Xat servers.

36. On November 8, 2015, an unknown third party gained root access to Xat's main server through 100TB (the "Second Cyberattack").

37. On information and belief, the unknown third party gained access to Xat's server during the Second Cyberattack through social engineering.

38. On information and belief, during the Second Cyberattack, the unknown third-party accessed Xat's proprietary log files, databases and source code, and erased system log files from Xat's server.

39. As a result of the First and Second Cyberattacks (the "Cyberattacks"), Xat has incurred damages in excess of at least $500,000, including:

a. The costs of containing the Cyberattacks;

b. The value of data deleted, lost, or stolen by an unknown third party;

c. Costs associated with reporting the Cyberattack to the appropriate authorities, including law enforcement and the United Kingdom's Information Commissioner's Office;

d. Lost revenue and profit as a result of shutting down Xat's website from November 4-19, 2015, while Xat addressed the Cyberattacks;

e. Costs of rebuilding Xat's website after the Cyberattacks; and

f. Legal costs and attorneys' fees.

FIRST CAUSE OF ACTION
(Gross Negligence)

40. Xat incorporates all other paragraphs of this Complaint.

41. 100TB failed to observe even slight care when it granted unknown third party access to Xat's servers in spite of repeated warnings from Xat that an unknown third-party was attempting to gain access to Xat's servers.

42. 100TB failed to observe even slight care when it turned on or failed to turn off Xat's server(s) after the First Cyberattack in spite of Xat's request.

43. 100TB failed to observe even slight care when it disabled two-factor authentication on Xat's servers despite Xat's request and in light of the prior attempts by an unknown third-party to access Xat's servers.

44. 100TB's conduct summarized in the foregoing three paragraphs is a gross deviation from the standard of care that an ordinary person would exercise given the circumstances.

45. 100TB owed Xat a duty to grant access to Xat's servers to Xat only and to comply with Xat's repeated requests to guard against the Cyberattacks, to turn off Xat's servers after the First Cyberattack, and not to disable two-factor authentication.

46. 100TB breached its duties to Xat by, among other things, granting an unknown third-party access to Xat's server(s).

47. As a result of 100TB's breach, Xat has sustained significant damages, including those identified above.

48. Xat's damages include the damages identified above and any claims asserted by its customers and/or regulatory authorities against Xat as a result of the Cyberattacks.

SECOND CAUSE OF ACTION
(Breach of Contract)

49. Xat incorporates all other paragraphs of this Complaint.

50. The MSA is a valid and enforceable contract.

51. Xat performed its obligations under the MSA by, among other things, making all payments due under the MSA prior to the Cyberattacks.

52. 100TB breached the MSA by, among other things, allowing an unknown third-party to commit the Cyberattacks.

53. As a result of 100TB's breach of the MSA, Xat has sustained damages, including those described above, and any claims asserted by its customers and/or regulatory authorities against Xat as a result of the Cyberattacks.

54. Pursuant to Paragraph 9 of the MSA, Xat is entitled to indemnity from 100TB for any claims or expenses, including costs and attorneys' fees, incurred in defending any claims asserted against Xat, as a result of the Cyberattacks.

THIRD CAUSE OF ACTION
(Unjust Enrichment)

55. Xat incorporates all other paragraphs of this Complaint.

56. Xat conferred a benefit upon 100TB, which included the purchase of services from 100TB since October 13, 2008.

57. 100TB appreciated and had knowledge of the benefit that Xat conferred upon 100TB.

58. 100TB accepted the benefit conferred by Xat under circumstances that make it inequitable for 100TB to retain such benefit without compensating Xat for the damages caused by the Cyberattacks, which include those identified above.

FOURTH CAUSE OF ACTION
(Equitable Indemnification)

59. Xat incorporates all other paragraphs of this Complaint.

60. Xat has incurred significant costs to remedy and avert any harm to its customers or any third-party whose information may have been exposed during the Cyberattacks, including costs of cooperating with the appropriate authorities and governmental agencies investigating the Cyberattacks.

61. 100TB is liable to any third-party whose information may have been exposed during the Cyberattacks.

62. Xat is entitled to be equitably indemnified by 100TB for all costs, including attorneys' fees, incurred as a result of any claims asserted by any third-party whose information was or may have been exposed during the Cyberattacks, and for any costs incurred in responding to the Cyberattacks or cooperating with the authorities and governmental agencies investigating the Cyberattacks.

PRAYER FOR RELIEF

WHEREFORE, Xat demands that judgment be entered against 100TB as follows:

1. Judgment in an amount to be proven at trial, inclusive of general and special damages, including (a) lost profits, (b) lost business opportunities, (c) damages for harm to Xat's business reputation, (d) lost operating revenue for the dates Xat had to shut-down its servers to address the Cyberattack, (e) compensation for the cost and time spent addressing the Cyberattack, and (f) any penalties assessed against Xat as a result of the Cyberattack.

2. An order requiring 100TB to indemnify Xat for any claims related to the Cyberattacks asserted by any third party, including any claims asserted by any regulatory authority or any individual or entity whose information was or may have been exposed during the Cyberattacks, and for any costs and attorneys' fees incurred by Xat related to any of the foregoing; and,

3. Xat's reasonable experts' and attorneys' fees and other costs and expenses incurred in this civil action or as a result of the Cyberattacks.

DATED June 28, 2016.

HOLLAND & HART LLP

/s/ Romaine C. Marshall
Romaine C. Marshall
Engels J. Tejeda

Plaintiff's Address:

Xat.com Limited
c/o Romaine Marshall
HOLLAND & HART LLP
222 South Main Street, Suite 2200
Salt Lake City, Utah 84101

8525137_3